Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions To	)	GN Docket No. 13-111
Combat Contraband Wireless Device	)	
Use in Correctional Facilities	)	FCC 17-25
	)	

CELL COMMAND, INC.'S COMMENTS
IN RESPONSE TO THE COMMISSION'S
FURTHER NOTICE OF PROPOSED RULEMAKING

Cell Command, Inc. ("Cell Command")[1], by and through its attorneys, respectfully submits these Comments in response to the Commission's May 18, 2017 Further Notice of Proposed Rulemaking ("*FNPRM*") and request for additional comments in the above-referenced proceeding. *See* 82 Fed. Reg. 22780 (May 18, 2017).

INTRODUCTION

The Federal Communications Commission (FCC) has the unique opportunity and dire responsibility to solve this public safety crisis once and for all. Now that technology exists for a comprehensive, cost-effective solution, the FCC must act and must resist those arguments that basically rest upon the concept that it hasn't been done this way before. The failure to act in the face of a solution would be an abdication of the FCC's statutory responsibility to preserve the safety of life and property.

As the Commission has correctly concluded, "[t]he use of contraband wireless devices in correctional facilities to engage in criminal activity poses a significant and growing security challenge to correctional facility administrators, law enforcement authorities, and the general

[1] Cell Command was formerly known as Try Safety First.

public." *FNPRM* ¶ 1. The FCC's record is replete with evidence and data that leaves no question about the threat of contraband devices and the devastating effect that they have had on law enforcement and American society. If anything, the Commission's language vastly understates the serious, epidemic nature of this public safety crisis, since new reports arrive almost daily of cell phone use to run criminal enterprises and gang activities from prison, to perpetrate attacks on correctional personnel, and to intimidate or kill witnesses.[2] Once, prison walls protected the public from felons; now, with contraband cell phones, there are no walls, and only the FCC can ensure the safety of the public again.

This ever-growing, serious threat to public safety necessitates a comprehensive solution that will completely disable *all* functionality on *all* wireless devices (except for 911 connectivity), not interfere with devices external to the facility, be backward and forward compatible, require no on-site staff monitoring, be legal, and be available at an affordable price.

The only technology that provides a comprehensive solution is continuous wave beacon (CW beacon) technology, as presented in Cell Command's Cell Warden system, comprised of two major components. First, software is embedded (by the manufacturer or pushed via update by the carrier) into the firmware of all cell phones. Second, the hardware beacons are installed in the specific areas of the correctional facilities where cell phone possession and use are prohibited. When activated, the beacon emits a specialized, non-interfering signal on the carrier control

[2] *See, e.g.* C. Roldán (2017, June 13), "34 indicted in meth trafficking operation run from state prisons." *The State* [South Carolina] (http://www.thestate.com/news/local/crime/article155841254.html); D. Holtmeyer (2017, May 26), "California man led Northwest Arkansas meth ring from prison, officials say." *Northwest Arkansas Democrat Gazette,* (http://www.nwaonline.com/news/2017/may/26/california-man-led-northwest-arkansas-m/); E. Leland and G. Off (2017, May 31), "Blood gang leader used prison cellphone to order hit on prosecutor's father." *The Charlotte Observer* (http://www.charlotteobserver.com/news/local/crime/article152334207.html); B. Bailey (2017, May 21), "Irish mob allegedly tries to silence witnesses in Oklahoma City shootout." *The Oklahoman NewsOK* (http://newsok.com/article/5549749); WXIA-TV (2017, May 18 11:33 AM), "Convicted felon threatens to kill undercover narcotics agent, gets more time." *WXIA-TV Channel 11 Atlanta* (http://www.11alive.com/news/local/convicted-felon-threatens-to-kill-undercover-narcotics-agent-gets-more-time/440783925).

channel. Cell phones with the CW beacon software recognize the signal, sound an alarm and shut down all cellphone functionality, rendering all memory and communications function useless.[3] The beacons are tamper-proof and, if moved without authorization, an alert of attempted tampering is sent to the correctional facility and memory in the beacon is automatically wiped.

Unfortunately, the other systems, such as the managed access, detect-and-disable, and jamming technologies discussed in the *FNPRM* and by some commenters, are not viable solutions to the contraband wireless device public safety threat. None of them provide a ubiquitous solution that disables all functionality on all wireless devices. As new generations of cell phones come out, managed access and other systems become less effective and must be updated with expensive upgrades. Additionally, each of them – particularly detect-and-disable – will require substantial Commission oversight and ongoing involvement of carriers, correctional facilities and/or system operators. These technologies are generally offered at unaffordable prices for correctional facilities, which usually operate on budgets with little room for excessive expenditures.

As detailed below, CW beacon technology[4] is the ***only*** technology available today that provides this comprehensive solution to completely disable all functionality of all wireless devices, while still permitting a user to connect to 911 emergency services. In the case of Cell Command's Cell Warden, this is done at an affordable cost. Indeed, Cell Command is committed to licensing its technology to device and beacon manufacturers on fair, reasonable and non-discriminatory terms. The cost per wireless device would be pennies. The hardware beacons are small, hardened and vastly less expensive to correctional facilities compared to every other solution. Further, Cell Warden operates with no on-site staff monitoring, no ongoing involvement of carriers and

[3] Cell phones without the software would not remain so for long. Any time that the cellphone connects to the network, it would receive the software along with other system updates automatically.

[4] Cell Command's continuous wave beacon technology has the registered trademark of Cell Warden®. However, the technology is licensable on FRAND terms (fair, reasonable and non-discriminatory) as discussed below.

correctional facilities, and with little to no Commission oversight or enforcement required. Once the Cell Warden software is installed on wireless devices and the beacon hardware deployed in the correctional facility, Cell Warden operates essentially as a "set it and forget it" solution for the Commission, the correctional facility, and carriers. It is also the only solution that is compatible with existing *and* future technologies, particularly the anticipated 5G rollout. As wireless technologies change and improve, Cell Warden will be updated over the air.

The FCC has traditionally avoided designating technology, deferring to the marketplace. The singular exception has been in matters of public safety, where the marketplace does not operate to sufficiently protect lives and property. Certainly, that is the case with contraband cellphones.

For these reasons, as well as those detailed below, Cell Command respectfully requests that the Commission exercise its authority under Section 332, Part 15 as well as its ancillary authority to designate CW beacon technology to defeat contraband wireless devices in correctional facilities and then to work with carriers, manufacturers and correctional officials on a voluntary regime for implementation of the technology within two (2) years from the date of issuance.

DISCUSSION

I. THE ATTRIBUTES OF A COMPREHENSIVE SOLUTION

To truly eliminate the threat to public safety caused by contraband wireless devices, the Commission must adopt a solution with the following attributes:

1. ***The Solution Must "Brick" the Phone***. The only effective solution is one that disables all functionality on a wireless device, as the Commission has recognized. *See FNPRM* ¶ 19 ("We seek to ensure that any disabling process will *completely disable* the contraband device itself and render it unusable, not simply terminate service to the device as the Commission had originally proposed in the" initial May 1, 2013 Notice of Proposed Rulemaking, FCC 13-58,

78 Fed. Reg. 36469 ("*NPRM*")) (emphasis added). Merely disabling voice and text functionality is insufficient, as inmates will remain able to use the device's other functions to engage in criminal activity and/or to harass victims and their family members. For example, inmates will still be able to communicate with their co-conspirators via e-mail or other internet applications over WiFi networks. As an additional example, inmates will use the camera function on the phone to take pictures of handwritten or other messages with instructions in furtherance of a criminal enterprise, with the phone or the SIM card then passed on directly to a co-conspirator during a visit or through another intermediary.

2. ***The Solution Must Work on All Phones.*** In order to be effective, the solution must be ubiquitous and work on *all* wireless devices. If it does not, inmates and their co-conspirators will identify the devices that will still work, and use those devices to continue criminal business as usual.

3. ***The Solution Must Be Affordable for Correctional Facilities.*** As the comments in this proceeding have demonstrated, correctional facilities often have budget constraints and are unable to spend significant funds on a technological solution to combat the contraband wireless device problem. *See e.g.*, June 8, 2016 Letter from Chairman Wheeler to Governors Haley, Daugaard, Deal, Pence, Bentley, Bryant, Rickets, LePage, Dalrymple, and Herbert ("The record also indicates that the cost of these technologies is a concern and that state and local funding limitations may have impeded wide-spread deployment."). Therefore, any solution that is adopted must not only be comprehensive, it must be available at an affordable price.

4. ***The Solution Must Not Interfere with Devices Outside of the Facility.*** For both legal and practical reasons, the adopted solution cannot interfere with devices external to the

correctional facilities. Such interference would be illegal and, moreover, would potentially create a separate public safety concern by disabling or hampering the wireless devices of citizens residing in proximity to the correctional facility.

5. ***The Solution Must Be Reliable, Secure and Extremely Resistant to Hacking or Tampering.*** The adopted solution must have been designed, executed and operated with strong encryption, anti-tampering protocols and the automatic capability of wiping all memory and functionality if moved without authority. It must have strong cybersecurity protections both from intrusion and from insider threats.

6. ***The Solution Must Be Backward and Forward Compatible.*** The adopted solution must not only be compatible with today's technology, it must also be compatible with future technologies. As the industry and technology evolves, the solution needs to be able to evolve with it. Technical updates and upgrades must be able to be made quickly and efficiently to the adopted solution.

7. ***The Solution Must Not Require Any On-Site Staff Monitoring.*** For both practical and cost reasons, the adopted solution must function solely with remote monitoring rather than personnel on-site at the correctional facility. On-site personnel cost money and, further, could be potentially intimated or otherwise compromised by inmates to assist them in avoiding the solution.

8. ***The Solution Must Be Legal.*** Obviously, any solution that is adopted must comply with applicable laws including, but not limited to, laws requiring the transmission of 911 calls and texts and laws prohibiting signal jamming.

II. MANAGED ACCESS, JAMMING AND DETECTION SYSTEMS ARE NOT VIABLE SOLUTIONS

The *FNPRM* indicates that "[a]s a general matter, there are primarily two categories of technological solutions currently deployed today in the U.S. to address the issue of contraband wireless device use in correctional facilities: Managed Access and detection." *FNPRM* ¶ 2. Some commenters also advocate for the use of jamming systems. While these technologies provide some capability to address the contraband wireless device problem, each also has inherent limitations that render them unacceptable solutions.

A. Managed Access Systems are Technologically Fatally Flawed and Prohibitively Expensive

Managed Access Systems have several inherent limitations that render them unsuitable as a comprehensive solution. First, a Managed Access System does not disable the entire functionality of the wireless device. Functions such as camera usage and, potentially, internet access through the use of WiFi may still be used by inmates and prisoners to engage in criminal activities and further criminal enterprises. The Commission correctly recognized this significant limitation in the *FNPRM*, concluding that "some of the technologies discussed," including Managed Access Systems, "could prevent an inmate from placing a call, but they may not prevent the inmate from using the phone for taking videos or otherwise sharing or disseminating information that itself could pose a threat to public safety." *See FNPRM* ¶ 53. This limitation, by itself, renders Managed Access Systems an unviable solution.

Second, Managed Access Systems will not work on all wireless devices. Indeed, most, if not all Managed Access Systems have difficulty detecting devices operating on an LTE network. Further, as the comments point out, Managed Access Systems can "be circumvented by offenders using family, friends, or other means to register numbers with the service managing system." July

15, 2013 Comments of the Oklahoma Corrections Professionals, at 1. Another means of circumvention is for inmates to have multiple SIM cards.

Third, Managed Access Systems are extremely expensive for correctional institutions, as the comments from correctional facilities, public safety personnel and others in this proceeding confirm. *See, e.g.*, June 19, 2017 Comments of the Tennessee Department of Correction, at 5 ("Currently, managed access solutions are complicated and expensive to implement with costs exceeding one million dollars per site and are ineffective.") (received by the Commission on June 13, 2017); Aug. 23, 2013 Reply Comments of The American Correctional Association, at 2 ("MAS have their limitations and are quite cost prohibitive to implement on a broad scale."); July 18, 2013 Comments of Network Communications International Corp. ("NCIC"), at 2 ("NCIC has found Managed-Access Systems to be a cost-prohibitive (about $1,000,000 in total for the average 500 bed jail) solution for most county and city governments"); July 18, 2013 Comments of the American Correctional Association (Managed Access Systems "are not without their complications nor are they particularly cost-effective to correctional agencies"). Indeed, costs for Managed Access Systems can range from $1.0 million to $5 million per facility depending on its size[5] just for the initial installation, with yearly monitoring, upgrade and other fees being charged to the facility thereafter, which themselves can be exorbitant.

Fourth, Managed Access Systems pose the serious risk of interfering with the wireless signals of innocent citizens in the communities surrounding the correctional facility, creating a significant threat to public safety separate and apart from the contraband wireless devices themselves. *See* CAL. COUNCIL ON SCIENCE & TECH., THE EFFICACY OF MANAGED ACCESS

[5] *See, e.g.*, J. Johnson (2014, Feb. 8), "Baltimore jail cracks down on contraband cellphones." *The Washington Post* (https://www.washingtonpost.com/local/md-politics/baltimore-jail-cracks-down-on-contraband-cellphones/2014/02/08/9db98a48-901f-11e3-b46a-5a3d0d2130da_story.html?utm_term=.1435bb0191dd).

SYSTEMS TO INTERCEPT CALLS FROM CONTRABAND CELL PHONES IN CALIFORNIA PRISONS (May 2012), at 19 ("[I]f the prison is in or near a populated area, this RF leakage [caused by Managed Access Systems] could be *highly disruptive* to cell phone usage by the non-prison population. Among other things, this disruption could greatly reduce the capability of public safety professionals to serve the community's needs or the general public's ability to access a 911 operator.") (https://ccst.us/publications/2012/2012cell.pdf).

Fifth, Managed Access Systems are inflicted with obsolescence problems, as they are not forward compatible and cannot be updated quickly or efficiently. For example, the California Department of Corrections and Rehabilitation installed Managed Access Systems in 18 of its facilities and thereafter concluded that the systems were not working due to significant problems with upgrades and the inability of the systems to block certain wireless transmissions. *See* K. Broder (2015, Dec. 25), "New, but not Unexpected, Technology Derails State's Plan to Squelch Prison Cellphones." (http://www.allgov.com/usa/ca/news/top-stories/new-but-not-unexpected-technology-derails-states-plan-to-squelch-prison-cellphones-151225?news=858050), *AllGov California*. Consistent with the experience in California, Managed Access Systems will not be capable of timely updates once carriers upgrade to 5G. Indeed, the upgrade of every Managed Access System in the country to accommodate 5G devices will take a significant amount of time and will cost a significant amount of money and manpower. Further, this assumes that each Managed Access System provider is currently planning for the 5G rollout and developing the necessary updates.

Sixth, as the *FNPRM* demonstrates, Managed Access Systems require significant Commission oversight as well as significant involvement of carriers, correctional facilities, and system operators. Specifically, each Managed Access System operator would first have to

negotiate a spectrum lease agreement with each carrier covering the geographic location of each correctional facility. While the Commission has adopted Rules that seek to expedite and streamline this process[6], the carriers and the system operators still must negotiate and (hopefully) agree on the terms of each lease for each correctional facility, which must then be submitted to the Commission for authorization. *See Final Rules Notice* ¶¶ 8, 49. To the extent that the parties are unable to agree, the Commission must attempt to resolve the stalemate after the parties have completed a briefing process. *See id.* ¶ 49. The Commission itself has acknowledged that if even one carrier fails to negotiate in good faith, the Managed Access System will not be effective. *See id.* Even with the streamlined process set up by the Commission's recently promulgated Final Rule, significant administrative burdens remain that will delay attempts to solve the contraband wireless device problem using Managed Access Systems. Moreover, Managed Access Systems require substantial monitoring and other oversight by correctional facility staff who are usually already overworked. *See e.g.* July 15, 2013 Comments of the Oklahoma Corrections Professionals, at 1 ("Intercepting and reporting of non-registered numbers – even streamlined – could be labor intensive."); CAL. COUNCIL ON SCIENCE & TECH., THE EFFICACY OF MANAGED ACCESS SYSTEMS TO INTERCEPT CALLS FROM CONTRABAND CELL PHONES IN CALIFORNIA PRISONS (May 2012), at 20 ("Current MAS technologies require significant human intervention and operational action due to a complete lack of automated feedback of operational performance.") (https://ccst.us/publications/2012/2012cell.pdf).

In short, Managed Access Systems are not an acceptable solution for resolving the threat to public safety caused by contraband wireless devices.

---

[6] *See In the Matter of Promoting Technological Solutions To Combat Contraband Wireless Device Use in Correctional Facilities,* GN Docket No. 13-111; FCC 17-25, Final Rule, 82 Fed. Reg. 22742 (May 18, 2017) ("*Final Rules Notice*").

B. Jamming and Geo-Fencing Technologies are Not Viable Solutions

The *FNPRM* also seeks comments on geo-fencing (*FNPRM* ¶ 50), while certain commenters advocate wireless signal jamming. "Radio signal jamming is the purposeful disruption of electronic devices, equipment, or systems via radio frequency interference." *NPRM* at 12 ¶ 18. "A radio signal jamming device transmits on the same radio frequencies as wireless devices and base stations, disrupting the communication link between the device and the network base station, and rendering any wireless device operating on those frequencies unusable." *Id.*

As with Managed Access Systems, jamming and geo-fencing also have several significant limitations. First and foremost, jamming is illegal except in certain limited circumstances. *See id.* ¶ 19.

Second, jamming and geo-fencing also have the real potential to interfere with legitimate wireless devices operating within the range of the jamming system. As the FCC itself recognizes, "[w]hen used to disrupt wireless devices, radio signal jammers cannot differentiate between contraband devices and legitimate devices, including devices making 911 calls." *Id.* ¶ 18. "Radio signal jammers block all wireless communications on affected spectrum bands." *Id.* Legalizing jammers in America opens the door to other and more illicit use, possibly by criminals or terrorists. In this regard, jamming and geo-fencing systems are unnecessarily and dangerously over-inclusive.

Third, jamming and geo-fencing systems are also under-inclusive, as they do not disable *all* functions of the contraband device, such as the camera.

Fourth, jamming systems can cost between $350,000 and $1.2 million per facility just for the installation, with accompanying upgrade and other fees being imposed on the facility thereafter.

Fifth, jamming systems, like Managed Access Systems, generally require on-site staff monitoring.

Sixth, as with Managed Access Systems, jamming and geo-fencing systems will not be equipped for timely updates to accommodate the 5G rollout, leaving inmates with newer 5G devices unfettered use of all functions to engage in and orchestrate criminal behavior.

In short, even if jamming systems were deemed legal, they will still not constitute a comprehensive solution to the contraband wireless device public safety threat.

C. The Detect-and-Disable System and Procedures Envisioned in the *FNPRM* Are Fatally Flawed for a Number of Reasons

The *FNPRM* also discusses detection as one of the technologies currently being used to address the contraband wireless device problem. *FNPRM* ¶ 2. "Detection systems are used to detect devices within a correctional facility by locating, tracking, and identifying radio signals originating from a device." *FNPRM* ¶ 3. "[D]etection systems have evolved with the capability of transmitting radio signals to not only locate a wireless device[], but also to obtain device identifying information." *Id.*

In the *FNPRM,* the Commission seeks "comment on a process whereby CMRS licensees would disable contraband wireless devices in correctional facilities detected by an eligible [Contraband Interdiction System (CIS)] when they receive a qualifying request from an authorized party." *FNPRM* ¶ 12.[7] The *FNPRM* envisions a complex process for this proposed detect-and-disable system, requiring significant and ongoing involvement of the Commission, wireless

[7] Managed Access System providers are expressly excluded from disabling contraband wireless devices through their systems unless they request authorization from the Commission. *FNPRM* ¶ 12 ("We clarify that CIS systems operating solely to prevent calls and other communications from contraband wireless devices, described in the *Notice* as MAS [Managed Access Systems], would not be subject to these eligibility criteria, unless the department of corrections/CIS provider seeks to use the information received from such a system to request, through Commission rules, contraband wireless disabling.").

carriers, the system operator, and correctional facility staff. First, the Commission seeks comment on whether it should determine in advance whether a CIS meets threshold standards "for eligibility to be the basis for a subsequent qualifying request for device disabling," including proposed performance criteria to determine such eligibility. *Id.* ¶ 20. Next, the Commission seeks comment on the qualifying request itself, including whether the request must be transmitted by the Commission to the carrier once it is received from a Designated Correctional Facility Official ("DCFO"), or whether the request can be transmitted directly from the DCFO to the carrier. *Id.* ¶ 22. Once the request is received by the carrier (from whomever transmits it), the carrier will need to verify the accuracy of the information transmitted and potentially make a determination on whether to involve the customer before a decision is made on disabling. *Id.* ¶ 30. Then there is the issue of how long it will take the carrier to make the decision to either disable the device or not. *Id.* ¶ 33. If the carrier wrongly refuses to disable the device, then the inmate or criminal can continue to use it.

The detect-and-disable system envisioned by the Commission is complicated and time-consuming, and requires the ongoing involvement and decision-making of several different entities. While this proposed system arguably could disable service to some contraband devices, it, like Managed Access and jamming systems, has several significant limitations that prevent it from adequately resolving the contraband wireless device problem.

First, the inmate will be able to use all functionality of the contraband device up to the time the carrier disables service to it – if the carrier is able ***and*** agrees to do so.

Second, even after the carrier disables whatever service it is able to, the inmate could use other functions of the phone that cannot be disabled by the carrier to commit further crimes, as the Commission correctly recognized. *See FNPRM* ¶ 53 ("some of the technologies discussed" in the

FNPRM, including detection, "could prevent an inmate from placing a call, but they may not prevent the inmate from using the phone for taking videos or otherwise sharing or disseminating information that itself could pose a threat to public safety."). Indeed, we are unaware of any technology being used by the carriers that would enable them to completely disable *all* functions and memory on a wireless device.

Third, there is still the chance that the person who smuggled the device into the facility is the same one that will be in charge of making the termination request, potentially reducing the likelihood that the termination request will even be made.[8]

Fourth, as demonstrated above, the detect-and-disable system envisioned in the *FNPRM* requires substantial involvement and coordination of several players, including that of overtaxed and short-staffed correctional facilities. *See* July 15, 2013 Comments of the Oklahoma Corrections Professional, at 1 ("Detection technology is not the answer as this option requires staff to operate the device, which is problematic considering corrections officers in Oklahoma are already required to work 60 hours per week due to short-staffing.").

Fifth, as the comments from some of the wireless carriers demonstrate, there remain several administrative and legal hurdles to the approval and implementation of a detect-and-disable system. While there is a dire need for a solution to the contraband wireless device public safety threat, the proposed detect-and-disable solution still "raises a number of concerns and questions that cannot be answered at this time given the lack of experience with such requests and information about the volume of termination requests carriers might receive." July 18, 2013 Comments of Verizon Wireless, at 2. These questions and concerns include, but are not limited

[8] *See, e.g.*, Leland & Off (2017, May 31), "Blood gang leader used prison cellphone to order hit on prosecutor's father." *The Charlotte Observer* (http://www.charlotteobserver.com/news/local/crime/article152334207.html); P. Brown, (2016, Feb. 12), "'Staggering corruption': 46 correctional officers charged in years-long drug-trafficking sting." *CNN* (http://www.cnn.com/2016/02/11/politics/fbi-georgia-correctional-drug-trafficking/index.html).

to: (1) the accuracy of the identification (i.e., whether the device is in fact a contraband device and, if so, whether it is actually that of a subscriber to the subject carrier's network) (*see id.* at 6); (2) the security of the information provided to the carrier (i.e., whether the information conveyed by the authorized requester is secure) (*see id.* at 7); (3) the timing of the disabling (*see id.* at 7-8); and (4) liability protection for the carrier in the event it inadvertently disables the service of a non-contraband device. *See id.* at 8; *see also FNPRM* ¶¶ 7-8. Because the answers to these questions still remain unknown, certain commenters contend that the FCC should require that service terminations for contraband devices be done only pursuant to a court order, at least initially. *See e.g.* July 18, 2013 Comments of Verizon Wireless, at 9; *see also FNPRM* ¶ 7. "Should experience demonstrate that a court order process is too slow or overly burdensome on prison officials or their Solutions Providers, the Commission can revisit the issue and consider a different process once all parties gain more experience with service terminations and once more detection systems are deployed." July 18, 2013 Comments of Verizon Wireless, at 9; *see also* July 18, 2013 Comments of CTIA – The Wireless Association®, at 12 (to the extent that the FCC adopts CellAntenna's detect-and-disable proposal, carriers should only be required to terminate service pursuant to an order from a court of relevant jurisdiction).

Sixth, detect-and-disable systems are, like Managed Access Systems, prohibitively expensive for correctional facilities, ranging between $300,000 and $1,000,000 ***per facility*** for initial installation, plus yearly monitoring, upgrade and other fees. This amount does not include the internal cost that each carrier would incur in receiving, investigating and responding to each request for disablement from correctional facilities.

Seventh, as with Managed Access and jamming and geo-fencing systems, detect-and-disable systems will not be equipped for timely updates to accommodate the 5G rollout, giving inmates with the newer phones complete, and uninterrupted functional use of the device.

For all of these reasons, detect-and-disable systems are not the solution to the contraband wireless device public safety threat.

III. CW BEACON SYSTEMS ARE THE *ONLY* COMPREHENSIVE SOLUTION

As demonstrated above, the Managed Access, jamming/geo-fencing, and detect-and-disable systems discussed by the FCC will not completely disable the functionality of contraband wireless devices, will involve a multitude of lease negotiations between system operators and each carrier for each correctional facility with no guarantee of agreement being reached on terms, will require a substantial amount of human intervention and involvement from multiple parties, and/or will implicate legal and administrative issues that hinder or prevent their adoption and implementation. What is needed is a solution that is ubiquitous, disables all contraband cell phone functionality (save for 911), and which involves minimal human intervention.

CW beacon technology, as developed by Cell Command's Cell Warden, provides that solution. This technology is comprised of a two part system – one part software and one part hardware. The software component consists of what is known as CCI Prison Protocol, which is to be loaded onto the firmware of all wireless phones in the United States. With respect to existing phones, the software will be loaded through an over-the-air firmware update from the carrier (the quickest method) or through a website set up by Cell Command that will be linked to the manufacturer and carrier websites. New phones will have the software installed during manufacture.

The hardware component – known as the Protocol Trigger Device for Prisons ("PTDP") – is a unique precision range transmitter/beacon with a one (1) to twenty (20) meter range. These devices are strategically placed inside the prison fences and buildings to broadcast a prison protocol trigger signal. All functionality of cell phones with the CCI Prison Protocol software – except 911 capabilities – will be disabled once inside the prison fence line and in range of the broadcast trigger signal.

More specifically, when a cell phone is first powered up, the Cell Warden software will scan first for a PTDP. If an active PTDP is found, the mobile device will identify its exact geographical location and then cross reference the device in order to apply proper operation in compliance with the applicable law for that jurisdiction to any phone operating inside a defined "Restricted Safety Zone" within the correctional facility. If no active PTDP is found, the phone operates normally. As the phone continues to scan (usually every 20 to 30 seconds) to ensure it is operating across the best or preferred network using the best or preferred base station tower, the scan will always include a search for an active PTDP and, if one is found, the contraband cell phone's functionality will be completely disabled except for 911 calls.

Cell Warden is the only current technology that completely disables all of a wireless device's functionality – including voice, text, e-mail, Wi-Fi, and camera/video – while permitting 911 calls to connect. This technology does so without tracking, listening to, or recording any activity on the cell phone. Cell Warden is also the only current technology that disables all functionality on *all* wireless devices, regardless of manufacturer.

Moreover, Cell Warden accomplishes complete disablement with hardly any administrative oversight by the FCC and with no involvement by carriers or the correctional facility after installation. Once the software is installed on wireless devices and the beacon

hardware deployed in the correctional facilities, Cell Warden operates as "set it and forget it." There is no complicated time-consuming process of transmitting a request to a carrier followed by a carrier's investigation into the request and subsequent decision on it. There is no need for administrative oversight or enforcement by the FCC of an ongoing relationship between carriers, correctional facilities and system operators because the Cell Warden system operates without their involvement after installation. Indeed, the solution requires no on-site monitoring and, as discussed above, the beacons are secure and tamper-proof. The correctional facility will only receive a notification if one of the beacons is moved without authorization and, in that event, the beacon's memory is automatically wiped. Additionally, the range in which the beacon system operates prevents any interference with devices outside of the facility.

Furthermore, Cell Warden will be remarkably more affordable than the other technological alternatives for the correctional facilities that wish to use it. While Cell Command itself will not be building the component parts of its system, it has committed to licensing its technology on fair, reasonable and non-discriminatory ("FRAND") terms to any industry participant that wishes to manufacture the components for their own compatible CW beacon system. For an average-sized correctional facility, the current cost for off-site monitoring is estimated to be approximately $36,000 per year. Additionally, unlike Managed Access, jamming/geo-fencing, and detect-and-disable systems, Cell Warden is compatible with existing and future technologies, including the anticipated 5G rollout (i.e., it is backward and forward compatible). As wireless technologies advance and improve, Cell Warden software can be updated over-the-air to stay fully compatible, and at *no additional cost*.

When compared to the other solutions discussed in the *FNPRM*, Cell Warden is confirmed to be the only platform that meets *all* eight attributes of a comprehensive, ubiquitous solution to the public safety threat caused by contraband wireless devices.

Additionally, several correctional facilities have submitted comments encouraging the Commission to adopt or approve geo-fencing and signal jamming as a means to combat contraband wireless devices. *See e.g.,* June 19, 2017 Comments of the Tennessee Department of Corrections, 6. As demonstrated above, geo-fencing and signal jamming are neither comprehensive nor necessarily inexpensive solutions. The Cell Warden solution, however, is ubiquitous and will be available at an affordable price for the correctional facilities that wish to use it.

The evidence demonstrates that the only effective solution to the public safety threat caused by contraband wireless devices is Cell Command's Cell Warden technology.

IV. THE COMMISSION'S LEGAL AUTHORITY TO FIND THAT CW BEACON TECHNOLOGY IS THE ONLY CURRENT, COMPREHENSIVE UBIQUITOUS SOLUTION

The *FNPRM* correctly acknowledges that "beacon-based technologies [like Cell Warden] would function effectively only if all wireless carriers perform a system update to include the software for all existing and future wireless devices, and all mobile device manufacturers include the software in all devices." *FNPRM* ¶ 54. The Commission seeks comment on whether this solution would "require legislation to ensure that all wireless carriers and wireless device manufacturers include the software in the wireless devices[.]" *Id.* "In the absence of legislation, how would the Commission ensure wireless carrier and device manufacturer cooperation and pursuant to what authority would the Commission be acting?" *Id.*

Cell Command does ***not*** advocate for mandatory implementation of CW beacon technology, but we provide information on the FCC's authority in response to the *FNPRM*'s

questions. As demonstrated below, the Commission already has the authority to ensure that all wireless carriers and wireless device manufacturers include beacon software in wireless devices. This authority is found in Section 332, Part 15 as well as the Commission's ancillary authority.

A. The FCC's Section 332, Part 15 Authority

The FCC has broad authority under Section 332 to regulate the spectrum over which wireless devices operate in order to promote the safety of life and property. More specifically, 47 U.S.C. § 332 provides, in pertinent part, as follows: "In taking actions to manage the spectrum to be made available for use by the private mobile services, the Commission shall consider, consistent with section 151 of this title, whether such actions will . . . promote the safety of life and property." 47 U.S.C. § 332(a)(1).

The Federal Government, several States and the FCC itself have all concluded that there is an overriding public interest in preventing prisoners from using wireless devices to further a criminal enterprise from within correctional facilities. *See FNPRM* ¶ 1; *NPRM* (released May 1, 2013) ¶¶ 1, 6. While a few correctional facilities achieved some initial success in testing or using a Managed Access System (*see NPRM* ¶ 15), as described above, California's did not. Indeed, California's expensive experiment with Managed Access Systems – cited by the Commission in its original 2013 *NPRM* (*see id.*) – subsequently failed. These systems are not capable of disabling all functionality of contraband cell phones, require multiple carrier/operator lease agreements, require ongoing Commission and correctional facility oversight and monitoring, and are expensive. Moreover, the great majority of correctional facilities have not implemented any technological solutions to combat this problem, either because of cost or other resource limitations.

In May of last year, ten (10) Governors wrote to the Commission encouraging the FCC to reevaluate the FCC's regulations regarding contraband cell phones. *See* May 23, 2016 Letter to

Chairman Wheeler from then Governor Mike Pence (IN), Governor Nikki Haley (SC) *et al*. In April, then-Commissioner, now Chairman Pai held a field hearing in Columbia, South Carolina on combating the public safety threats posed by inmates' use of contraband cell phones. *See* then-Commissioner Pai's Field Hearing on Contraband Cellphones, April 6, 2016. And the FCC understands that it must take action. *See Unofficial announcement of Commission action*, February 29, 2016, Comment of then-Commissioner Pai ("We cannot let inmates treat prison as just another base of operations for criminal enterprises. We need to act.").

The FCC already regulates mobile devices under Part 15 of its Rules, which sets out the standards under which intentional, unintentional, or incidental radiators may operate. *See generally* 47 C.F.R. Part 15. Mobile devices, as intentional radiators (*see* 47 C.F.R. § 15.3(o)), are subject to Part 15's equipment authorization requirements. Specifically, unlicensed intentional radiators must be verified pursuant to the procedures in 47 C.F.R. Part 2, Subpart J. *See* 47 C.F.R. § 2.901 *et. seq.*

Part 15 was adopted pursuant to the Commission's Section 302a authority, which is not limited exclusively to preventing harmful interference, but also authorizes the Commission to take action in "the public interest" to "govern[] the *interference potential* of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means . . . ." 47 U.S.C. § 302a (emphasis added). While Section 302a refers to "interference," the language is exceedingly broad in that it covers Commission action, consistent with the public interest, governing interference potential. It is not limited to harmful interference, and it is not limited to actual interference; rather, it extends to interference "potential." *Id.*

Any Commission action consistent with the public interest which impacts the interference potential of a Part 15 device is within the scope of Section 302a. Thus, a technology that limits

the operation of a wireless device (i.e. its ability to emit radio signals) in a particular environment may be authorized through Commission action under Section 302a.

The legislative history of Section 302a acknowledges this well understood fact. Prior to the passage of Section 302a, the Commission only had the power "to prohibit the use of equipment or apparatus which causes interference to radio communications." 1968 *U.S. Code Cong. and Admin. News,* p. 2487. In other words, the FCC had no authority to attempt to regulate the interference potential of devices at the manufacturing level, but rather could only take action against a user of equipment when an actual instance of harmful interference had occurred. *See id.* at pp. 2487–2488. It was the Senate's view that it was more equitable to place the burden of equipment compliance on the manufacturer in the first instance. *See Id.*

The Commission has broad discretion in making policy determinations through, *inter alia,* the issuance of policy statements, and addressing the issue of contraband wireless device use in prisons is squarely within the Commission's delegated authority and public safety responsibilities. *See American Radio Relay League, Inc. v. F.C.C.,* 617 F.2d 875, 881 (D.C. Cir. 1980) ("The Commission has broad discretion in making policy determinations . . .;" denying a challenge to FCC rules prohibiting the manufacture and sale of certain amplifiers in order to combat the problem of radio interference with television reception); 47 U.S.C. § 151 - Purposes of chapter; Federal Communications Commission created (providing that the Commission was created for, among others, "the purpose of promoting safety of life and property through the use of wire and radio communications").

The Commission's authority to regulate wireless devices is further evidenced in the Commission's July 17, 2015 Notice of Proposed Rulemaking in *In the Matter of Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency*

Equipment, Request for the Allowance of Optional Electronic Labeling for Wireless Devices, ET Docket No. 15-170, 80 Fed. Reg. 46900-01 (Release July 21, 2015) ("Wireless Device Notice"). The purpose of the Wireless Device Notice was to update the rules governing the evaluation and approval of RF devices.[9] The Wireless Device Notice proposes "rules [that] would require any RF device that uses software to control its defining parameters to incorporate software security features that permit only those parties that have been authorized by the manufacturer to make changes to the device's technical parameters." Wireless Device Notice ¶ 20.

The security features proposed by the FCC in the *NPRM* and *FNPRM* in this proceeding implicate similar policy goals and similar technology that Cell Command now urges the FCC to address and effectuate through the issuance of a policy statement. The FCC recognizes that it may require manufactures to implement safety features related to wireless communication. These same features can be used to solve the serious public safety threat caused by contraband wireless device use in prisons.

B. The FCC's Ancillary Authority

While Section 302a alone provides sufficient authority for the Commission to issue a policy statement finding that CW beacon technology is the only current technology that satisfies the criteria for a comprehensive, ubiquitous solution to the contraband wireless device public safety threat, the Commission may also utilize its ancillary authority to do so. *See generally* 47 U.S.C. § 154(i).

[9] An RF device is any device that is capable of emitting RF energy by radiation, conduction, induction or other means. As defined in FCC rules, this includes radio communication transmitting devices and any device that includes a part or component that can act as an RF device. *See* 47 C.F.R. § 2.801. While RF devices generate RF energy, many devices do not generate it intentionally – that is, they are not communications devices but they generate RF emissions as a byproduct of their design. Such devices are defined as incidental or unintentional radiators. *See* 47 C.F.R. § 15.1.

The Commission has the authority to issue policy statements to effectuate the goals and provisions of the Act even in the absence of an explicit grant of regulatory authority if the policy statement is reasonably ancillary to the Commission's specific statutory powers and responsibilities. *See* 47 U.S.C. § 154(i) (providing that the "Commission may perform *any and all acts* . . ., not inconsistent with this chapter, as may be necessary in the execution of its functions.") (emphasis added).

In order for the Commission to act under its ancillary jurisdiction, two conditions must be met. First, the subject of the action must be covered by the Commission's general grant of jurisdiction under Title I of the Act. Second, the subject of the action must be "reasonably ancillary to the effective performance of the Commission's various responsibilities." *See United States v. Southwestern Cable Co.*, 392 U. S. 157 (1968).

Both of these conditions are satisfied here as: (1) mobile devices (intentional radiators) are covered by the FCC's Title I general jurisdictional grant; and (2) regulating those devices to protect the safety of the public from contraband wireless devices is, at a minimum, reasonably ancillary to the performance of the Commission's responsibilities. Indeed, the statutorily proscribed policy goal of "promoting safety of life and property" is directly at issue. Both Section 151 – "Purposes of chapter; Federal Communications Commission created" and Section 154 – "Use of communications in safety of life and property" detail broad policy goals to promote public safety. *See* 47 U.S.C. §§ 154(o) ("For the purpose of obtaining maximum effectiveness from the use of radio and wire communications in connection with safety of life and property, the Commission shall investigate and study all phases of the problem and the best methods of obtaining the cooperation and coordination of these systems."); 332(a)(1) ("In taking actions to manage the spectrum to be made available for use by the private mobile services, the Commission shall

consider, consistent with section 151 of this title, whether such actions will . . . promote the safety of life and property.").

In other words, the FCC's broad ancillary authority – in addition to the other authority discussed above – empowers the Commission to continuously investigate and regulate new public safety problems created by technological advances in mobile technologies and the continuing increase in their use by inmates to carry on criminal enterprises from within the confines of correctional facilities. Issuance of a policy statement finding that CW beacon is the only current technology that satisfies the criteria for a comprehensive, ubiquitous solution to the contraband wireless device public safety threat is not only authorized, it is imperative.

C. The FCC Has Previously Mandated a Single Technology In Order to Protect the Safety of the Public – Here it Can and Should Issue a Policy Statement Finding that a Single Technology is the Only Effective Solution

A major mission of the FCC has been addressing the appalling lack of interoperability among first responders licensed by the FCC. Through various proceedings, programs such as Project 25[10], and advisory committees such as the iterative Communications Security, Reliability and Interoperability Council (CSRIC), the goal of interoperability in the pursuit of public safety has been frustratingly elusive. In response to the tragic events of 9/11, followed by the disaster caused by Hurricane Katrina in 2005, the FCC saw an opportunity to achieve interoperability if a new public safety broadband network were instituted and the Commission unanimously adopted "rules to guide development of a nationwide interoperable public safety broadband network," i.e., FirstNet. *In the Matter of Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band,* PS Docket No. 06-229, Third Report and Order and Fourth Further Notice of Proposed Rulemaking ¶ 5 (Released Jan. 26, 2011). "[T]o ensure nationwide

[10] National Task Force on Interoperability, *Why Can't We Talk: Working Together to Bridge the Communications Gap to Save Lives*, p.57 (February, 2005).

interoperability, [the Commission] mandate[d] that all public safety broadband networks adopt LTE as a common technology platform." *Id.* The reason that the Commission mandated LTE as the common technology platform was because, *inter alia,* previous efforts to implement public safety over narrowband had proven "to be elusive" and the time had come for the Commission to declare one technology platform in order to ensure that public safety personnel throughout the country could communicate with each other. *See id.* ¶ 9. In other words, interoperability across first responders scattered throughout the United States was necessary to protect the public safety, yet the variety of different communication systems being used by first responders made interoperability, at best, very difficult and, at worst, impossible. Mandating one communication technology (LTE) resolved this problem.

CW beacon technology similarly solves – completely – the public safety threat imposed by contraband wireless device use in the nation's prisons and jails. Under the Commission's existing Rules, it clearly has the authority to issue a mandate in this proceeding requiring carriers and wireless device manufacturers to implement CW beacon technology. However, Cell Command believes that, at this point, such a mandate is unnecessary. Rather, the Commission should designate, pursuant to the authority discussed herein and for public safety purposes, CW beacon technology for combatting contraband wireless devices in prisons, finding that it is the only current comprehensive, ubiquitous solution to the contraband wireless device public safety threat. The FCC should call upon carriers and wireless device manufacturers to work together with the FCC on a voluntary basis to develop a regime for implementation of the technology within two (2) years from the date of issuance.

Dated: June 19, 2017 Respectfully submitted,

__/s/__James Arden Barnett, Jr_____
James Arden Barnett, Jr., Esq.
Rear Admiral USN (Retired)

__/s/__Stephen R. Freeland_____
Stephen R. Freeland, Esq.

__/s/__Ian Volner_____
Ian Volner, Esq.

__/s/__Christopher Boone_____
Christopher Boone, Esq.

Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
(202)-344-4000

Its Attorneys